Cryptology ePrint Archive: Report 2011/346

Strongly Secure One Round Authenticated Key Exchange Protocol with Perfect Forward Security

Hai Huang

Abstract: This paper investigates the two-pass authenticated key exchange protocol in the enhanced Canetti-Krawczyk (eCK) with perfect forward security. Currently, there exist no authenticated key exchange protocols which are provably secure in eCK model and meanwhile achieve perfect forward security against active adversary in one round.

We propose a new two-pass authenticated key exchange protocol which enjoys following desirable properties. \textbf{First}, our protocol is shown secure in the eCK model under the gap Diffie-Hellman (GDH) assumption. Moreover, our protocol does not use the NAXOS transformation, the drawback of which will be discussed in the introduction. \textbf{Second}, under the same assumption, we prove that our protocol achieves perfect forward security against active adversary in one round.

To the best of our knowledge, our proposal is first two-pass (one round) AKE protocol provably secure in the eCK model and achieving perfect forward security against active adversary.

Category / Keywords: cryptographic protocols /

Publication Info: To some conference, submmision date: May 15, 2011

Date: received 27 Jun 2011

Contact author: haihuang1005 at gmail com